VASU SINGLA

Google Scholar Link - geHpT2IAAAAJ
Website - vasusingla.github.io
Email ID - vsingla@cs.umd.edu

RESEARCH STATEMENT

My current research interests has been focused on robust and responsible AI. Recently, I've worked on uncovering, and mitigating the safety and privacy risks of generative models, specifically text to image generative models.

EDUCATION

University of Maryland, College Park August 2021 - Dec 2024 (Expected)
Ph.D. in Computer Science
Advisor: Prof. Tom Goldstein, Prof. David Jacobs

University of Maryland, College Park August 2019 - May 2021
M.S in Computer Science GPA: 4.0/4.0

Punjab Engineering College, Chandigarh July 2014 - June 2018
B.Tech. + Minors GPA: 8.2/10

SELECTED PUBLICATIONS

Visit my Google Scholar Link for all publications
∗ denotes equal contribution

- From Pixels to Prose: A Large Dataset of Dense Image Captions — Under Review
  V. Singla*, K. Yue*, S. Paul, R. Shirkavand, M. Jayawardhana, A. Ganjdanesh, H. Huang, A. Bhatele, G. Somepalli, T. Goldstein
- PUP 3D-GS: Principled Uncertainty Pruning for 3D Gaussian Splatting — Under Review
  A. Hanson, A. Tu, **V. Singla**, M. Jayawardhana, M. Zwicker, T. Goldstein
- A Simple and Efficient Baseline for Data Attribution on Images — NeurIPS ATTRIB Workshop
  V Singla, P. Segura, M. Goldblum, J. Geiping, T. Goldstein
- Understanding and Mitigating Copying in Diffusion Models — NeurIPS 2023
  G. Somepalli, **V. Singla**, M. Goldblum, J. Geiping, T. Goldstein
- What Can We Learn from Unlearnable Datasets? — NeurIPS 2023
  Pedro Sandoval-Segura, **Vasu Singla**, Jonas Geiping, Micah Goldblum, Tom Goldstein
- Learning with noisy labels using low-dimensional model trajectory — NeurIPS DistShift Workshop
  V. Singla, T. Koike-Akino, M. Brand, K. Parsons, S. Aeron, Y. Wang
- Diffusion Art or Digital Forgery? Investigating Data Replication in Diffusion Models — CVPR 2023
  G. Somepalli, **V. Singla**, M. Goldblum, J. Geiping, T. Goldstein
- Autoregressive Perturbations for Data Poisoning — NeurIPS 2022
  P. Segura*, **V. Singla***, J. Geiping, M. Goldblum, T. Goldstein, D. Jacobs
- Poisons that are learned faster are more effective — CVPR AROW Workshop
  P. Segura, **V. Singla**, L. Fowl, J. Geiping, M. Goldblum, D. Jacobs, T. Goldstein
- Shift Invariance Can Reduce Adversarial Robustness — NeurIPS 2021
  V. Singla*, S. Ge*, R. Basri, D. Jacobs

- Low Curvature Activations Reduce Overfitting in Adversarial Training ICCV 2021
  V. Singla, S. Singla, S. Feizi, D. Jacobs

RESEARCH EXPERIENCE

Google Research July 2024 - Current
Student Researcher

- Working on multi-modal foundation models for climate change.

Cruise Research Jan 2023 - May 2023
Research Intern

- Working on developing novel applications of diffusion models for Autonomous Vehicle systems.
- Trained image-conditioned inpainting diffusion models for internal datasets.

Mitsubishi Electric Research Labs June 2022 - Aug 2022
Research Intern

- Proposed new optimization algorithms to improve accuracy on datasets with noisy labels. Explored the role of data quality and labels on the robustness of ML systems.

Apple June 2021 - Aug 2021
Research Intern

- Selected as the **top-8 out of 100s of interns** to present work to the **Senior VP of AI/ML Organization at Apple**.
- Proposed new data augmentation techniques to boost performance on low-resource accents for Automatic Speech Recognition models.

University of Maryland January 2020 - Present
Research Assistant

- Worked with Prof. Tom Goldstein on safety and privacy risks of generative models.
- Worked with Prof. David Jacobs on adversarial examples.

Indian Institute of Technology (IIT), Bombay January 2019 - July 2019
Research Staff

- Developed a novel system for automated symbol detection, text detection and object association in documents for structured parsing, analysis and information retrieval.

AWARDS

NeurIPS 2023 Travel Award, ICLR 2021 Travel Award, UMD Dean's Fellowship

ACADEMIC SERVICE

Grants - Co-wrote and won Amazon Research Award Grant for Building Safer Diffusion models, winning over 50K USD in funding.
Reviewer Conferences - CVPR 2022, ECCV 2022, CVPR 2023, ICCV 2023, NeurIPS 2023, ICLR 2024, NeurIPS 2024
Reviewer Journals - CVIU, Pattern Recognition Letters
Volunteer Services - ICML 2021, NeurIPS 2023, Peer Mentoring Service @ UMD